INTERVIEW REQUEST

Applicant notes that Applicant's attorney, Robert G. Hartman, made several written and oral requests to interview this matter with the Office. Examiner Kendall agreed to conduct a telephonic interview on March 20, 2008, at 3:00pm EST. However, Applicant attorney's and the Examiner were unable to connect for an interview at that time. Nevertheless, Applicant's attorney will again attempt to discuss this matter with the Examiner following the filing of this Response. Although the Examiner and Applicant's attorney have thus far been unable to connect, Applicant sincerely thanks Examiner Kendall for agreeing to speak with Applicant's attorney. Applicant's attorney looks forward to discussing this matter with the Examiner in the near future.

REMARKS

Claims 1, 8, 11, 13, 20, 23-25, 28, 30, and 32 are currently amended. Claim 2 is canceled herein. Claims 1, 3, 6-13, 16-20, 23-25, 27-28, and 30-33 are pending and are listed below. In view of the foregoing amendments and the following remarks, Applicant respectfully requests that this application be allowed and forwarded on to issuance.

§ 103 REJECTIONS

Claims 1-3, 6-13, 16-18, 20, 23-25, 27-28, and 33 stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Patent No. 6,199,204 to Donohue (hereinafter, "Donohue") in view of U.S. Patent No. 7,000,247 to Banzhof (hereinafter, "Banzhof").

Claim 19 stands rejected under 35 U.S.C. §103(a) as being obvious over Donohue in view of Banzhof in further view of U.S. Patent No. 5,930,504 to Gabel (hereinafter, "Gabel").

Applicant respectfully traverses the rejections. Nevertheless, for the sole purpose of expediting allowance and without conceding the propriety of the Office's rejections, Applicant has amended each of the independent claims.

Applicant notes that much of the subject matter added to each of the independent claims is similar to the subject matter previously recited in now-canceled claim 2. As such, Applicant respectfully requests that the Office enter these amendments in response to this Amendment after Final.

THE CLAIMS

Claim 1 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (added language underlined):

- receiving a binary signature at a server computing device, the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file located on a client computing device;
- receiving a security patch at the server computing device;
- identifying, from the server computing device, the particular vulnerable binary file located on the client computing device based on the binary signature, the client computing device being remote from the server computing device;
- updating, from the server computing device, the particular vulnerable binary file located on the client computing device with the security patch; and
- wherein the identifying of the particular vulnerable binary file located on a client computing device comprises comparing the bit pattern that is associated with the security vulnerability in the particular vulnerable binary file against bit patterns of binary files located on the client computing device, and wherein the updating of the particular vulnerable binary file occurs if a bit pattern of the particular vulnerable binary file exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.

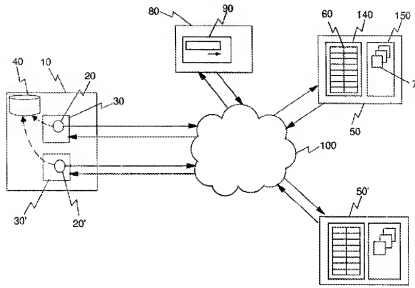
In making out a rejection of claim 1 before this amendment, the Office states that the combination of Donohue and Banzhof renders the claim obvious. Applicant respectfully disagrees for at least the reasons discussed in Applicant's previous Response. Nevertheless, for the sole purpose of expediting allowance and without conceding the propriety of the Office's rejections, Applicant has amended this claim as shown above.

In addition to those arguments previously presented, Applicant respectfully submits that the cited references at least fail to disclose or suggest:

> receiving a binary signature at a server computing device, *the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file located on a client computing device*; and
>
> wherein the identifying of the particular vulnerable binary file located on a client computing device comprises *comparing the bit pattern* that is associated with the security vulnerability in the particular vulnerable binary file *against bit patterns of binary files located on the client computing device*, and *wherein the updating of the particular vulnerable binary file occurs if a bit pattern of the particular vulnerable binary file exactly matches the bit pattern of the binary signature that is associated with the security vulnerability.*
>
> Claim 1 (emphasis added).

Donouhue

Donohue describes an updater agent that is associated with a computer program on a client computer and that accesses relevant network locations to download and install updates to the agent's associated program on the client computer. The agent downloads and installs the updates if those updates satisfy predefined update criteria of the updater agent. Donohue, abstract. As Donohue's Fig. 1 illustrates, the updater component 20 is installed in system memory of a conventional network-connected computer system 10 and functions to perform updates on that computer. Id. at col. 6, lines 3-6.



In order to so perform updates on the computer, the updater agent first initiates a search for available updates to the particular software product, providing to one or more search engines 90 as search arguments the product identifier and product version release number obtained at install time. This search should identify the relevant Web site 140 on which update information is available. A URL identifying the relevant Web site 140 for update information is returned 210 to the updater component as a result of the search. Id. at col. 8, lines 25-43.

The updater component then uses the URL to access the list 60 and downloads a file 160 comprising the portion of the list 60 of available updates which relates to the particular product. Each file 160 contains message digests (e.g. MD5) which are digitally signed. *The retrieved file 160 is then analyzed 240 using a digital signature checking algorithm to verify that the file 160 represents the correct software updates list for the particular software product, and that the file has not been tampered with since signing.* Id. at col. 8, lines 44-55.

The updater component then performs on the local computer system a comparison between the current installed software product's identifier and release

number and the listed available updates in the retrieved file 160. This comparison determines possible growth paths from the current to updated versions, but these possible growth paths are then compared 260 with predefined update criteria, and any possible paths which do not satisfy the update criteria are discarded. Thus, the updater component determines whether it is possible to migrate from a current software product to the available new versions and whether it is possible to apply patches to the current version under the currently agreed license terms and conditions. Id. at col. 8, line 64 to col. 9, line 9 (emphasis added).

In short, the Donohue updater component downloads a list of possible updates and compares this list with product identifiers and release numbers of the software currently installed on the computer in order to identify possible updates.

Banzhof

Banzhof discusses a system and process for addressing computer security vulnerabilities. The system and process includes aggregating vulnerability information on a plurality of computer vulnerabilities; constructing a remediation database of said plurality of computer vulnerabilities; constructing a remediation signature to address the computer vulnerabilities; and deploying said remediation signature to a client computer. Banzhof, abstract.

However, in order to deploy the remediation signatures to a client computer, Banzhof describes that the client user, typically an IT person or other computer security personnel, *is given the opportunity to select which vulnerabilities should be remediated. Generally, the selection is made by reviewing the information regarding vulnerabilities, proposed signatures, and profiles.* The selection and review may be made for each computer or by

vulnerability. For example, a particular computer could be selected not to receive any remediation, perhaps because the computer does not pose a significant security risk, the vulnerabilities on the computer are not significant, the processes running on the computer cannot be interrupted for remediation, etc. Alternatively, a particular vulnerability could be deselected for all target client computers, such that the vulnerability would not be remediated on any of the target computers, perhaps because the vulnerability does not pose a sufficient security risk, the remediation signature is deemed too risky, etc. Once the user has selectively managed which vulnerabilities will be remediated, the user can then select which computers will be approved to receive remediation in box. Id. at col. 9, lines 17-37.

In short, Banzhof teaches allowing a client user (e.g., an IT person) to determine whether or not to download a remediation signature with reference to a client computer's profile.

Applicant's Claim 1

As shown above, Applicant's claim 1 recites, in part:

> receiving a binary signature at a server computing device, *the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file located on a client computing device*; and
>
> wherein the identifying of the particular vulnerable binary file located on a client computing device comprises *comparing the bit pattern* that is associated with the security vulnerability in the particular vulnerable binary file *against bit patterns of binary files located on the client computing device*, and *wherein the updating of the particular vulnerable binary file occurs if a bit pattern of the particular vulnerable binary file exactly matches the bit pattern of*

the binary signature that is associated with the security vulnerability.

Claim 1 (emphasis added).

Applicant respectfully submits that neither Donohue or Banzhof (or the combination thereof) teaches or suggest at least this portion of Applicant's claim. As discussed above, the updater component of Donohue analyzes a *list* of possible updates to determine if the currently installed software on the computer should be updated. However, comparing a *mere list of updates* fails to teach or suggest "*comparing* ***[a] bit pattern*** that is associated with the security vulnerability in the particular vulnerable binary file ***against bit patterns of binary files*** *located on the client computing device*". Furthermore, Donohue's comparison of a list and a profile fails to teach or suggest "*wherein the updating of the particular vulnerable binary file occurs if* ***a bit pattern*** *of the particular vulnerable binary file* ***exactly matches the bit pattern of the binary signature*** *that is associated with the security vulnerability*".

Simply put, Donohue fails to teach or suggest comparing a "bit pattern" of a binary signature with a "bit pattern" of a binary file to look for an "exact[] match".

Also as discussed above, Banzhof describes a remediation process where an IT person may determine whether or not to update software with reference to a list of available updates and a profile of one or more client computers. However, this list/profile comparison fails to teach or suggest comparing a "***bit pattern***" of a binary signature with a ***"bit pattern" of a binary file***. Similar to Donohue, Banzhof simply fails to teach or suggest comparing bit patterns in hopes of finding an "exact[] match".

As such, Applicant respectfully submits that neither of the cited references teaches or suggests "receiving a binary signature at a server computing device, *the binary signature comprising a bit pattern that is associated with a security vulnerability in a particular binary file located on a client computing device*; and…wherein the identifying of the particular vulnerable binary file located on a client computing device comprises *comparing the bit pattern* that is associated with the security vulnerability in the particular vulnerable binary file *against bit patterns of binary files located on the client computing device*, and *wherein the updating of the particular vulnerable binary file occurs if a bit pattern of the particular vulnerable binary file exactly matches the bit pattern of the binary signature that is associated with the security vulnerability*", as recited in claim 1 (emphasis added).

For at least these reasons, Applicant respectfully submits that this claim stands allowable.

Claims 3 and 6-7 depend from claim 1 and, as such, the remarks made above in regards to claim 1 apply equally to these claims. The rejections of these claims are also improper as failing to show how the references of record teach or suggest, either singly or in combination, these claims' own recited features in combination with those recited in claim 1.

Independent claims 8, 11, 13, 20, 23-25, 28, 30, and 32 have each been amended in a manner similar to the amendment to claim 1 discussed immediately above. Therefore, Applicant respectfully submits that each of these claims stands allowable for at least reasons similar to those discussed above in regards to claim 1, in addition to the reasons previously submitted in Applicant's prior Response.

Dependent Claims 9-10, 12, 16-19, 27, 31, and 33 each depend from one of independent claims 8, 11, 13, 25, 30, and 32. As such, the remarks made above in regards to these independent claims apply equally to these dependent claims. The rejections of these dependent claims are also improper as failing to show how the references of record teach or suggest, either singly or in combination, these claims' own recited features in combination with those recited in each claim's respective base claim.

CONCLUSION

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully submitted,

Dated: _____ By: _____

Robert G. Hartman
Reg. No. 58,970
(509) 324-9256 ext 265